Published and Copyright (c) 1999 - 2013
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1522 06/07/13

~ Letter Re. Windows Red ~ People Are Talking! ~ Calling Out China!
~ Punishing Cyber Theft! ~ NH Approves Protection ~ Mass. Teen Freed!
~ Camino Is Discontinued ~ Foxconn & Mozilla Team ~ NSA "Surveillance"!

~ Turkey Arresting Twits ~ What To Expect at WWDC ~ No to Direct Access!

-* U.S. Cyber War Preparations! *-
-* Used Games Will Work on New Xbox One *-
-* Digging for [Fool's] Gold in New Mexico Dump *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"

Another week, another batch of weather anomalies! Last weekend, we had a heat wave. This weekend, we're encountering a tropical storm! Amazing. I don't know what's planned for next weekend, but the way things have been going, I'm not looking forward to any more extremes! Hopefully, your late Spring is going a lot better than we're experiencing on the east coast!

Until next time...

=~=~=~=

->In This Week's Gaming Section - Studio To Comb N.M. Landfill for Bad Atari Games!
Microsoft Says Used Games Will Work on Xbox One!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!

Studio To Comb N.M. Landfill for Bad Atari Games

A New Mexico city commission agreed to allow a Canadian studio to search a landfill where old, terrible Atari games are rumored to be buried.

Alamogordo commissioners decided last week that they will allow Fuel Industries to search the landfill for games, according to The Alamogordo Daily News. The company has offices in Ontario and Culver City, Calif.

One sought-after cartridge, the E.T. video game, is thought by some to be

among the worst video games of all time. Atari paid Steven Spielberg tens of millions of dollars to license the wildly popular 1982 movie's name, and the dud of a game caused the troubled company's worth to sink even further at the time.

The game has since developed a cult following.

The rumored Atari graveyard has long been a fascination of some who consider the commercial flop a part of video game history. It is believed that nine semi-trucks dumped the E.T. game and other Atari toys in the southern New Mexico landfill in 1983.

Alamogordo Commissioner Jason Baldwin says he played the Extra-Terrestrial game and it was horrible. There are listings for the game on eBay that run from under a dollar to more than $30.

Fuel Industries, a multimedia company, has been given six months to search the landfill. The company hopes to document the search.

Microsoft Says Used Games Will Work on Xbox One

Microsoft's upcoming Xbox One gaming console will be able to play used games, clearing up a worry among gamers and video game retailers such as GameStop, which trade in used games.

That means video games discs users buy will not be limited to one Xbox One device, and players can share or trade in the games they have bought for other used games, just as they have been able to do in the past.

Microsoft Corp. said in a blog post Thursday that it will not charge a fee to retailers, publishers or gamers for transferring their old games.

The Xbox One, which goes on sale later this year, will need to be connected online at least once every 24 hours to work. Some players had been concerned that the console was going to require a constant Internet connection.

Users will be able to access their games from other consoles through an online library after installing them on their primary device, but they will need to connect to the Internet at least every hour. They will be able to watch live TV and Blu-ray and DVD movies on the Xbox One without an Internet connection, Microsoft said.

Microsoft will give more details about the Xbox One next week at the E3 video game conference in Los Angeles.

=~=~=~=

With Troops and Techies, U.S. Prepares for Cyber Warfare

On the site of a former military golf course where President Dwight Eisenhower once played, the future of U.S. warfare is rising in the shape of the new $358 million headquarters for the military's Cyber Command.

The command, based at Fort Meade, Maryland, about 25 miles north of Washington, is rushing to add between 3,000 and 4,000 new cyber warriors under its wing by late 2015, more than quadrupling its size.

Most of Cyber Command's new troops will focus on defense, detecting and stopping computer penetrations of military and other critical networks by America's adversaries like China, Iran or North Korea.

But there is an increasing focus on offense as military commanders beef up plans to execute cyber strikes or switch to attack mode if the nation comes under electronic assault.

"We're going to train them to the highest standard we can," Army General Keith Alexander, head of Cyber Command, told the Reuters Cybersecurity Summit last month. "And not just on defense, but on both sides. You've got to have that."

Officials and experts have warned for years that U.S. computer networks are falling prey to espionage, intellectual property theft and disruption from nations such as China and Russia, as well as hackers and criminal groups. President Barack Obama will bring up allegations of Chinese hacking when he meets President Xi Jinping at a summit in California beginning on Friday - charges that Beijing has denied.

The Pentagon has accused China of using cyber espionage to modernize its military and a recent report said Chinese hackers had gained access to the designs of more than two dozen major U.S. weapons systems in recent years. Earlier this year, U.S. computer security company Mandiant said a secretive Chinese military unit was probably behind a series of hacking attacks that had stolen data from 100 U.S. companies.

There is a growing fear that cyber threats will escalate from mainly espionage and disruptive activities to far more catastrophic attacks that destroy or severely degrade military systems, power grids, financial networks and air travel.

Now, the United States is redoubling its preparations to strike back if attacked, and is making cyber warfare an integral part of future military campaigns.

Experts and former officials say the United States is among the best - if not the best - in the world at penetrating adversaries' computer networks and, if necessary, inserting viruses or other digital weapons.

Washington might say it will only strike back if attacked, but other countries disagree, pointing to the "Stuxnet" virus. Developed jointly by the U.S. government and Israel, current and former U.S. officials told Reuters last year, Stuxnet was highly sophisticated and damaged nuclear enrichment centrifuges at Iran's Natanz facility.

U.S. government officials frequently discuss America's cyber vulnerabilities in public. By contrast, details about U.S. offensive

cyberwarfare capabilities and operations are almost all classified.

Possible U.S. offensive cyber attacks could range from invading other nations' command and control networks to disrupting military communications or air defenses - or even putting up decoy radar screens on an enemy's computers to prevent U.S. aircraft from being detected in its airspace.

The shift toward a greater reliance on offense is an important one for a nation which has mostly been cautious about wading into the uncertain arena of cyberwar - in part because gaps in U.S. cybersecurity make it vulnerable to retaliation.

But former Homeland Security Secretary Michael Chertoff said the United States must be ready and should articulate - soon - what level of cyber aggression would be seen as an act of war, bringing a U.S. response.

"One of the things the military learned, going back to 9/11, is whether you have a doctrine or not, if something really bad happens you're going to be ordered to do something," he told the Reuters summit. "So you better have the capability and the plan to execute."

Reuters has learned that new Pentagon rules of engagement, detailing what actions military commanders can take to defend against cyber attacks, have been finalized after a year of "hard core" debate. The classified rules await Defense Secretary Chuck Hagel's signature, a senior defense official said.

The official would not give details of the rules but said, "they will cover who has the authority to do specific actions if the nation is attacked."

At Cyber Command, military officers in crisp uniforms mix with technical experts in T-shirts as the armed forces takes up the challenge of how to fend off cyber penetrations from individuals or rival countries.

Even as overall U.S. defense spending gets chopped in President Barack Obama's proposed 2014 budget, cyber spending would grow by $800 million, to $4.7 billion while overall Pentagon spending is cut by $3.9 billion.

Until its new headquarters is ready, Cyber Command shares a home with the U.S. National Security Agency (NSA), which for 60 years has used technological wizardry to crack foreign codes and eavesdrop on adversaries while blocking others from doing the same to the United States. Alexander heads both agencies.

"The greatest concentration of cyber power in this planet is at the intersection of the Baltimore-Washington Parkway and Maryland Route 32," said retired General Michael Hayden, a former CIA and NSA director, referring to NSA's Fort Meade location.

But NSA's role in helping protect civilian, government and private networks has been controversial - and is likely to come under greater scrutiny with this week's revelation that it has been collecting telephone records of millions of Verizon Communications customers under a secret court order.

A January report by the Pentagon's Defense Science Board gave a general picture of how the United States might exploit and then attack an adversary's computer systems.

In some cases, U.S. intelligence might already have gained access for

spying, the report said. From there, Cyber Command "may desire to develop an order of battle plan against that target" and would require deeper access, "down to the terminal or device level in order to support attack plans," it said.

Because gaining access to an enemy's computers for sustained periods without detection is not easy, "offensive cyber will always be a fragile capability," it said.

In cyberspace, reconnaissance of foreign networks is "almost always harder than the attack" itself because the challenging part is finding a way into a network and staying undetected, said Hayden, now with the Chertoff Group consulting firm.

Cyber Command's new Joint Operations Center, due to be complete in 2018, will pull disparate units together and house 650 personnel, officials said. Air Force, Army, Navy and Marine Corps components will be nearby and, a former U.S. intelligence official said, the complex will have power and cooling to handle its massive computing needs.

Those who have worked at Cyber Command say the atmosphere is a mixture of intensity and geek-style creativity. Military precision is present, but it is not unusual to see young civilian computer whiz kids with purple hair, a tie-dyed shirt and blue jeans.

"It's made to be a fun environment for them. These are people who are invested and want to serve their nation. But there is some military rigor and structure around all that - like a wrapper," said Doug Steelman, who was director of Network Defense at Cyber Command until 2011 and is now Chief Information Security Officer at Dell SecureWorks.

Cyber Command's growth and expanding mission come with serious challenges and questions.

For example, how to prevent U.S. military action in cyberspace from also damaging civilian facilities in the target country, such as a hospital that shares an electric grid or computer network with a military base?

And some doubt that the military can train many cyber warriors quickly enough. Alexander has identified that as his biggest challenge.

The former intelligence official said Cyber Command's new teams won't be fully ready until at least 2016 due to military bureaucracy and because it takes time to pull together people with the special skills needed.

"To be a good cyber warrior, you have to be thinking, How is the attacker discovering what I'm doing? How are they working around it?' ... Cyber security really is a cat and mouse game," said Raphael Mudge, a private cybersecurity expert and Air Force reservist. "That kind of thinking can't be taught. It has to be nurtured. There are too few who can do that."

Would-be cyber warriors go through extensive training, which can take years. A recruit with proven aptitude will be sent to courses such as the Navy-led Joint Cyber Analysis Course in Pensacola, Florida, a 6-month intensive training program.

The top 10 percent of JCAC's students will be selected for advanced cyber operations training, said Greg Dixon, a vice president at private KEYW Corp, which conducts intensive training classes.

The company can train a JCAC graduate to become an analyst in five weeks, but it takes 20 weeks to become a cyber operator. Dixon would not divulge what an operator would be capable of doing after graduation, but said it would be "a lot."

"They're going to pick the cream of the crop for the 'full spectrum cyber missions'," the former U.S. intelligence official said, using a euphemism for cyber offense.

Before a future cyber warrior can begin advanced training, he or she has to pass through the arduous security clearance process, which can take six to nine months for personnel who are not already cleared.

Troops earmarked for cyber warfare have found themselves washing floors, mowing lawns and painting at military installations as they bide time waiting for a clearance.

There is the concern about retaliation for a U.S. cyber attack. Some analysts say Iran increased its cyber capabilities after being infected with Stuxnet, which was revealed in 2010.

"The old saying, he who lives in a glass house should be careful of throwing stones ... but if the stone that you threw at someone, when you live in a glass house, is a stone that in some way they could pick back up and throw back at you, that's an even dumber idea," the defense official said. "We definitely think about that as one aspect of considering action."

U.S. Lawmakers To Introduce New Bill To Punish Cyber Theft

A day before Chinese President Xi Jinping visits the United States, three U.S. lawmakers plan to propose a new law that would punish hackers backed by China, Russia or other foreign governments for cyber spying and theft.

The new bill that would go after specific hackers from "offending nations" with "real consequences and punishments" will be introduced on Thursday by House of Representatives Intelligence Committee Chairman Mike Rogers, a Republican from Michigan, Democratic Representative Tim Ryan of Ohio and Republican Senator Ron Johnson of Wisconsin.

Rogers, whose office did not immediately release further details of the bill, leads cybersecurity efforts in Congress. He has co-authored a cybersecurity bill meant to ease sharing of cyber threat data between companies and the government that passed the House earlier this year.

President Barack Obama will meet China's Xi at a California summit this week and plans to tell him that Washington considers Beijing responsible for any cyber attacks launched from Chinese soil and that China must abide by international "rules of the road" on cybersecurity.

China has consistently denied U.S. accusations of cyber hacking and has insisted it is more a victim than a perpetrator.

The White House declined to specify what, if any, punitive measures the United States might take if Xi refuses to cooperate and the cyber threats persist.

"Cyber hackers from nation-states like China and Russia have been aggressively targeting U.S. markets, stealing valuable intellectual property, and then repurposing it and selling it as their own," Rogers' office said in announcing the plans for the bill's introduction.

The new bill will be the second such legislation taken up by Congress. A group of powerful senior senators last month introduced the Deter Cyber Theft Act to combat computer espionage and the theft of commercial data from U.S. companies.

The differences are for now unclear between the new Rogers bill to be introduced on Thursday and last month's Senate bill introduced by Democrats Carl Levin of Michigan and Jay Rockefeller of West Virginia, and Republicans John McCain of Arizona and Tom Coburn of Oklahoma.

The Senate bill requires the Director of National Intelligence to compile an annual report that includes a list of nations that engage in economic or industrial espionage in cyberspace against U.S. firms or individuals. The president would also be required to block imports of products containing stolen U.S. technology, among others.

The new bill is expected to face a challenge in Congress this year. A divided Congress has not approved much legislation in recent years, given a string of partisan fiscal battles.

Cyber Experts Say Calling Out China May Be Working

After years of quiet and largely unsuccessful diplomacy, the U.S. has brought its persistent computer-hacking problems with China into the open, delivering a steady drumbeat of reports accusing Beijing's government and military of computer-based attacks against America.

Officials say the new strategy may be having some impact.

In recent private meetings with U.S. officials, Chinese leaders have moved past their once-intractable denials of cyber espionage and are acknowledging there is a problem. And while there have been no actual admissions of guilt, officials say the Chinese seem more open to trying to work with the U.S. to address the problems.

"By going public the administration has made a lot of progress," said James Lewis, a cybersecurity expert at the Center for Strategic and International Studies who has met with Chinese leaders on cyber issues.

But it will likely be a long and bumpy road, as any number of regional disputes and tensions could suddenly stir dissent and stall progress.

On Wednesday, China's Internet security chief told state media that Beijing has amassed large amounts of data about U.S.-based hacking attacks against China but refrains from blaming the White House or the Pentagon because it would be irresponsible.

The state-run English-language China Daily reported that Huang Chengqing, director of the government's Internet emergency response agency, said Beijing and Washington should cooperate rather than confront each other in the fight against cyberattacks. Huang also called for mutual trust.

President Barack Obama is expected to bring up the issue when he meets with China's new president, Xi Jinping, in Southern California later this week. The officials from the two nations have agreed to meet and discuss the issue in a new working group that Secretary of State John Kerry announced in April. Obama's Cabinet members and staff have been laying the groundwork for those discussions.

Standing on the stage at the Shangri-La Dialogue security conference last weekend, Defense Secretary Chuck Hagel became the latest U.S. official to openly accuse the Chinese government of cyber espionage as members of Beijing's delegation sat in the audience in front of him. The U.S., he said, "has expressed our concerns about the growing threat of cyber intrusions, some of which appear to be tied to the Chinese government and military."

But speaking to reporters traveling with him to the meeting in this island nation in China's backyard, Hagel said it's important to use both public diplomacy and private engagements when dealing with other nations such as China on cyber problems.

"I've rarely seen that public engagement resolves a problem, but it's important," he said, adding that governments have the responsibility to keep their people informed about such issues.

The hacking issue also featured prominently over two days of meetings between the U.S. Chamber of Commerce and a leading Chinese trade think tank in Beijing.

"This is arguably the single most consequential issue that is serving to erode trust in the relationship," said Jeremie Waterman, the chamber's executive director for greater China. "Over time, it could undermine business support for U.S.-China relations."

According to Lewis and other defense officials familiar with the issue, China's willingness to engage in talks with the U.S. about the problem even without admitting to some of the breaches is a step in the right direction.

Cybersecurity experts say China-based instances of cyber intrusions into U.S. agencies and programs including defense contractors and military weapons systems have been going on since the late 1990s. And they went along largely unfettered for as much as a decade.

A recent Pentagon report compiled by the Defense Science Board laid out what it called a partial list of 37 programs that were breached in computer-based attacks, including the Terminal High Altitude Area Defense weapon, a land-based missile defense system that was recently deployed to Guam to help counter the North Korean threat. Other programs whose systems were breached include the F-35 Joint Strike Fighter, the F-22 Raptor fighter jet and the hybrid MV-22 Osprey, which can take off and land like a helicopter and fly like an airplane.

The report also listed 29 broader defense technologies that have been compromised, including drone video systems and high-tech avionics. The information was gathered more than two years ago, so some of the data are dated and a few of the breaches such as the F-35 had already become public.

According to U.S. officials and cyber experts, China hackers use gaps in software or scams that target users' email systems to infiltrate

government and corporate networks. They are then often able to view or steal files or use those computers to move through the network accessing other data.

Chinese officials have long denied any role in cyberattacks and insisted that the law forbids hacking and that their military has no role in it. They have also asserted that they, too, are often the victim.

Cyber experts say some of the breaches that emanate from Internet locations in China may be the product of patriotic hackers who are not working at the behest of Beijing’s government or military but in independent support of it.

The Chinese government’s control of the Internet, however, suggests that those hackers are likely operating with at least the knowledge of authorities who may choose to look the other way.

U.S. officials have quietly grumbled about the problem for several years but steadfastly refused to speak publicly about it. As the intrusions grew in number and sophistication, affecting an increasing number of government agencies, private companies and citizens, alarmed authorities began to rethink that strategy.

They were pressed on by cybersecurity experts including prominent former government officials who argued that using cyberattacks to steal intellectual property, weapons and financial data and other corporate secrets brought great gain at very little cost to the hackers. The U.S. government, they said, had to make it clear to the Chinese that continued bad behavior would trigger consequences.

In November 2011, U.S. intelligence officials for the first time publicly accused China and Russia of systematically stealing American high-tech data for economic gain.

That was followed by specific warnings about Chinese cyberattacks in the last two annual Pentagon reports on China’s military power. And in February, the Virginia-based cybersecurity firm Mandiant laid out a detailed report directly linking a secret Chinese military unit in Shanghai to years of cyberattacks against U.S. companies. After analyzing breaches that compromised more than 140 companies, Mandiant concluded that they can be linked to a unit that experts believe is part of the People’s Liberation Army’s cyber command.

The change in tone from the Chinese leaders came through during recent meetings with Gen. Martin Dempsey, chairman of the Joint Chiefs of Staff, and has continued, according to officials and experts familiar with more recent discussions with Chinese leaders.

Still, experts say that progress with the Chinese will still be slow and that it’s naive to think the cyberattacks will stop.

"This will take continuous pressure for a number of years," said Lewis. "We will need both carrots and sticks, and the question is when do you use them."

Turkey Is Now Arresting Dozens for Using Twitter

Freedom of speech is not high on the shifting priorities list of Turkish Prime Minister Recep Tayyip Erdogan. And after he chastised "every kind of lie on" Twitter and blamed almost everything else but his government for the outbreak of violence across his country at least 25 people have been arrested this week for messages of protest, perhaps centered on a few videos or one photo, that they've posted on the social network. "Nine of those arrested were detained in the city of Izmir. It remained unclear which comments on the microblogging site prompted the detentions," the Deutsche Presse-Agentur reported. As we explained on Tuesday night, the origin of social-media messages has been difficult to track down in the eight days of spreading resistance in Turkey, but the western coastal city of Izmir has been featured in several YouTube clips purportedly showed police delivering beatings to protesters.... (Warning: graphic.)

As the DPA notes, it's extremely unclear, given the chaos as misreporting out of the country, which pieces of social-media protest got these 25 people arrested or if their arrests are tied to more beyond, you know, free speech. Right now, of course, thousands upon thousands of Turks are tweeting messages speaking out against Ergodan, who said on Sunday that the violent uproar was due in large part to social media:

> There is a problem called Twitter right now and you can find every kind of lie there ... The thing that is called social media is the biggest trouble for society right now.

Protests continue to be organized on Twitter, and users have captured brutal scenes in person and shared them on platforms like Twitter, YouTube, and Facebook as any protester would do these days. But this movement and Erdogan's political pushback erupted because of the violence and the tear gas police used on environmentalists and protesters on May 28, not because of Twitter. That just raised the profile.

"Polis raided 38 addresses and took the ones they captured to the police station," reported CNN Turk (with a translation via Reddit). "Sixteen people are taken into custody for encouraging rebellion using social media and making propaganda ... It is reported that the number of people in custody may increase while the police is still questioning the ones taken into custody."

But again, it's remains almost completely unclear what these tweeters did or who these tweeters are reports only suggest that they furthered the protests from their accounts. The terms "encouraging rebellion" and "making propaganda" aren't really specific, and considering Erdogan's aversion to Twitter and protesters in general, those terms could be broad and encompass things like retweeting protest plans, or circulating photos of the violence. "If that s a crime, then we all did it," Ali Engin, a local representative from the opposition Republican People's Party (CHP) in Izmir, told the DPA.

If you look at tweets coming out of the country, a popular meme is getting passed around and it seems that people were arrested for tweeting this specific photo:

> Apparently 29 people were arrested in #Turkey for tweeting this photo of Turkish police assaulting two girls twitter.com/VOT99/status/3
>
> Voice of Turkey (@VOT99) June 5, 2013

That'd be troubling if true. But that hasn't been verified.

Perhaps more troubling is the free-speech crackdown that could follow, and

make Turkey’s moment so much different from and at once similar to the Arab Spring protests to which it’s already been compared: Could the Turkish government eventually crack down on text messages and phone calls? Will Turkey do what the Egyptian government did in 2011 and shut down the Internet and cell phone service? That didn’t exactly work then, and that’s unlikely to quell protesters now.

U.S. Intelligence Chief Says Surveillance Targets Non-U.S. Citizens

U.S. intelligence chief James Clapper said on Thursday the law that allows American government agencies to collect communications from internet companies only permits the targeting of "non-U.S. persons" outside the United States.

Responding to articles published by the Washington Post and Britain’s Guardian newspaper, Clapper, the director of national intelligence, said in a statement that the stories contained "numerous inaccuracies," but he did not offer any details.

The Post and Guardian reported that the U.S. government tapped directly into the servers of leading U.S. internet companies, allowing agents to examine emails, photos and other documents.

Microsoft Says Not Part of Broad Government Online Monitoring

Microsoft Corp said on Thursday it provides customer data to the U.S. government only when it receives a legally binding order and only on specific accounts, after the Washington Post reported U.S. security agencies had access to its central servers.

The Post reported on Thursday the U.S. National Security Agency and the FBI were "tapping directly into the central servers of nine leading U.S. Internet companies" - including Microsoft - through a highly classified program known as PRISM, extracting audio, video, photographs, emails, documents and connection logs.

Microsoft made no mention of the PRISM program in a statement released after the Post report, and denied it was part of any voluntary data collection mechanism.

"We provide customer data only when we receive a legally binding order or subpoena to do so, and never on a voluntary basis," Microsoft said in the emailed statement.

"In addition we only ever comply with orders for requests about specific accounts or identifiers. If the government has a broader voluntary national security program to gather customer data we don’t participate in it."

Facebook Denies Providing Government ’Direct Access’ to Servers

Facebook Inc said Thursday it does not provide any government agency with "direct access" to its servers, denying a central element of a Washington Post report.

The Post reported on Thursday that the U.S. National Security Agency and the FBI are "tapping directly into the central servers of nine leading U.S. Internet companies" through a highly classified program known as PRISM, extracting audio, video, photographs, emails, documents and connection logs.

"We do not provide any government organization with direct access to Facebook servers," Facebook Chief Security Officer Joe Sullivan said in a statement. "When Facebook is asked for data or information about specific individuals, we carefully scrutinize any such request for compliance with all applicable laws, and provide information only to the extent required by law."

Apple Denies Giving Government "Direct Access" to Servers

Apple Inc on Thursday said it does not provide any government agency with direct access to its servers, denying a key aspect of a Washington Post report.

The Post reported on Thursday that the U.S. National Security Agency and the FBI are "tapping directly into the central servers of nine leading U.S. Internet companies" through a highly classified program known as PRISM, extracting audio, video, photographs, emails, documents and connection logs.

"We have never heard of PRISM," Apple spokesman Steve Dowling said. "We do not provide any government agency with direct access to our servers, and any government agency requesting customer data must get a court order."

Asked whether Apple joined the NSA-FBI data collection program, Apple declined to comment beyond its brief statement.

The Washington Post reported that Apple held out for more than five years after PRISM enlisted its first corporate partner, in May 2007, for "unknown reasons."

NH Senate Approves Social Media Protections

New Hampshire’s Senate voted unanimously Thursday to prohibit bosses from requiring employees or job applicants to disclose user names or passwords to personal Facebook, Twitter or other social media or email accounts.

But the Republican-controlled chamber voted 13-11 along party lines to add an amendment on union contracts that could spell trouble when the bill goes back to the House to consider changes to the bill.

The bill would apply the ban to the workers’ personal accounts unrelated to the employer’s business. The bill does not prevent employers from enforcing workplace policies about company equipment.

The measure would not prohibit an employer from obtaining information in the public domain or prevent the employer from investigating whether the employee is complying with securities or financial laws based on the person’s personal website used for business purposes.

The House passed the bill in March, but the Senate amended it Thursday so the House must review the changes.

Democrats were upset the Republican majority added what they view is a "poison pill" to the bill the contents of a bill the Democratic House killed that gave a 10-member joint legislative committee power to approve cost items in collective bargaining contracts with state employee unions.

Senate Democratic Leader Sylvia Larsen of Concord objected the added provision could doom the social media provisions. The Senate passed the social media part of the bill unanimously, but added the contract provisions 13-11 along party lines.

Last year, six states California, Delaware, Illinois, Maryland, Michigan and New Jersey passed similar laws barring employers from requiring the disclosure of Facebook, Twitter or other account information, according to the National Conference of State Legislatures.

NCSL reports that legislation is pending in at least 35 states this year including New Hampshire. Arkansas, Colorado, New Mexico, Utah and Washington passed laws this year and bills have been sent to the governor in Oregon and Vermont.

Some states have similar laws to protect college students from having to grant access to social networking accounts, according to NCSL.

In their effort to vet job applicants, some companies and government agencies have started asking for passwords to log into a prospective employee’s accounts on social media sites, such as Facebook and Twitter. Critics call it an invasion of privacy akin to handing over the keys to the person’s house.

Sen. Donna Soucy, a co-sponsor of the New Hampshire bill, said employers can gain access to information about an employee or job applicant through social media accounts like Facebook that they otherwise could not legally obtain. She said people post personal information about themselves on Facebook, or others post on the person’s page. That information, she said, should be protected.

She said she had not heard of any New Hampshire employers demanding the information.

Soucy, D-Manchester, said employers can use information on social media accounts to discriminate, such as not interviewing someone whose Facebook picture shows the applicant to be obese when weight would not be required on the application.

Soucy said other people can post information on the person’s page that the person might not delete before a prospective employer saw it.

Allowing employers access to social media accounts also gives them access to others linked to the account, which could infringe on their privacy.

Massachusetts Teen Accused of Facebook Terror Post Freed

A Massachusetts teenager jailed a month ago for a Facebook post that suggested he could do worse than the Boston Marathon bombers was released, a court official said on Friday, after a grand jury refused to indict him.

Cameron D'Ambrosio was arrested on May 1 and accused of "communicating a terrorist threat." The 18-year-old aspiring rapper from Methuen, 30 miles north of Boston, posted lyrics online that included the words "a boston bombing wait till u see the shit I do."

The case sparked a viral online effort by rights activists to have him freed, and demonstrated the growing tension between law enforcement and free speech proponents after a spate of terror and school-violence incidents across the country.

Lawrence District Court Judge Lynn Rooney issued an order on Thursday to release D'Ambrosio after a grand jury chose not to indict, the court clerk's office said. An official at the county prosecutor's office was not available to comment.

"While today is a major victory for Cam, the chilling effect that this case has already had on free speech cannot be undone," said Evan Greer, of Boston's Center for Rights and Fight For The Future, which organized an online petition supporting D'Ambrosio that gathered 90,000 signatures.

Police had arrested D'Ambrosio after fellow students at Methuen High School alerted them of his Facebook posts. If D'Ambrosio had been convicted of the terrorism charge, he would have faced as many as 20 years in prison.

The case came weeks after twin bombs exploded at the finish line of the Boston Marathon on April 15, killing three people and injuring 264. Investigators said the attack was the work of two brothers of Chechen descent.

Some lawmakers have criticized the FBI's handling of the case, given that the older of the brothers, Tamerlan Tsarnaev, had been on a U.S. master list of potential terrorism suspects. Tamerlan was killed in a shootout with police days after the bombing and his younger brother Dzhokhar was wounded after a manhunt and is in prison for the crime.

Police are also under pressure to avoid a repeat of recent school shootings, including the Sandy Hook Elementary School shooting in Newtown, Connecticut last year in which 20 students and six school staff were killed.

"Law enforcement wants to preempt acts of violence before they occur," said Shirin Sinnar, assistant professor of law at Stanford University Law School. "The risk is that you sweep in people who had no intent to cause a crime."

Foxconn and Mozilla Are Collaborating To Develop 5 Devices for OEMs

Mozilla and Foxconn have officially announced a partnership and confirmed that the two firms are developing at least 5 new devices, including a tablet computer.

At a press conference today at Computex 2013 in Taipei, Li Gong, CEO of Mozilla Taiwan, and Young Liu, General Manager of Foxconn innovation Digital System Business Group, unveiled a new tablet prototype model designed for an unnamed OEM.

Further details remain scarce, as no specs or price points were revealed. However, in a Q&A session, Mozilla stated that it was optimistic that its HTML5 OS would help it position itself in both developed markets and emerging ones.

In addition to unveiling the tablet in question, Foxconn and Mozilla stated they are working on at least 5 devices, and stressed that their partnership wouldn t be limited to smartphones and tablets. Foxconn s broad portfolio, the firms stressed, put it in a prime position to extend Mozilla s OS into television screens or signage.

When asked what these developments meant for Foxconn s status as a brand, Li and Liu stated that Foxconn would remain a manufacturer, not a brand, and the purpose of the collaboration is to optimally integrate of Mozilla s OS with hardware. Details related to specs and marketing will be left to the OEMs.

The partnership marks a turning point as both firms attempt to move beyond their flagship products and services. Mozilla is continuing to push its vision for the mobile Web via its mobile OS which includes a starry array of partnerships while Foxconn is diversifying its business beyond manufacturing devices for consumer brands.

Last February at Mobile World Congress in Barcelona, the firm officially announced the mobile OS and deals with LG, ZTE, Huawei, and others to roll out devices to markets in Latin America and Europe.

Since then, the first manufacturer to bring the OS to physical reality was Geeksphone, the relatively unknown Spanish hardfirm which released developer versions of two smartphones in April. The Peak and Keone proved to be popular, with initially batches selling out in hours.

Foxconn, meanwhile, has made efforts to broaden its portfolio beyond making devices for Huawei, ZTE, and most famously, Apple. It was recently discovered that Apple s largest supplier is no longer Foxconn, but instead Pegatron.

Camino Browser Project Discontinued After Ten Years

Pour one out for Camino. The Mac-only browser, born a decade ago, is no longer under active development.

Camino was a free, open-source browser for the Mac, built on Mozilla s Gecko engine. Unlike other Mozilla-based browsers of its era, Camino featured a totally native OS X interface from day one. By contrast, Firefox has long used a cross-platform interface markup language, which to this day makes some Mac users feel that the app isn t quite Mac-like.

First launched in February 2002 as Chimera, Camino started as a project within Netscape; it was originally created by Dave Hyatt, who went on to join Apple s Safari team later that year, where he remains today. (Hyatt

also co-created Firefox.) Legal considerations later forced the name change to Camino.

One of the Chimera/Camino project s co-founders was Mike Pinkerton, who became the project s lead when Hyatt left for Apple. Pinkerton later moved onto Google, where he worked on Camino in his twenty-percent time. He also worked on Firefox, and is now part of the Chrome browser team.

On Camino s website, a message announced the browser s end of life, saying that it is no longer being developed, and we encourage all users to upgrade to a more modern browser. The page states that the browser is increasingly lagging behind the fast pace of changes on the web, and more importantly it is not receiving security updates, making it increasingly unsafe to use.

The page also reference s the Camino browser s impressive pedigree: Former Camino developers have helped build Chrome, Firefox, and Safari, concluding that the community that helped build [Camino] is still making the web better for Mac users.

The final released version of the browser is 2.1, which is still available for download.

Camino Reaches Its End

After a decade-long run, Camino is no longer being developed, and we encourage all users to upgrade to a more modern browser. Camino is increasingly lagging behind the fast pace of changes on the web, and more importantly it is not receiving security updates, making it increasingly unsafe to use.

Fortunately, Mac users have many more browsers to choose from than they did when Camino started ten years ago. Former Camino developers have helped build the three most popular Chrome, Firefox, and Safari so while this is the end of Camino itself, the community that helped build it is still making the web better for Mac users.

Thank you to all our loyal users, and to everyone who contributed in countless ways over the years to make Camino what it was.

iOS 7, Mac OS X Updates, MacBooks and More: What to Expect at Apple’s WWDC

It has been nearly nine months since Apple has held its last big event. In that time the company has suffered from some issues on Wall Street, been scrutinized for tax evasion and most recently defended its E-Book pricing against the Department of Justice.

But on Monday the maker of the iPhone and iPad will take the stage to focus on the future of its products at its annual Worldwide Developer’s Conference (WWDC). Held at the Moscone Center in San Francisco, the company will preview the next versions of its iOS operating system for the iPhone and iPad and the next version of Mac OS X.

We know those two things for sure, Apple CEO Tim Cook said so himself last

week. But the details of those new software platforms and some more products are shrouded in Apple's usual secrecy. As Monday's keynote event approaches, the rumors and speculation have come along with it. Here are a few of the things that Apple is expected to have been saving up for the big event, which ABCNews.com will be covering live at 10 a.m. PT / 1 p.m. ET.

No matter what else Apple shows at the event, the next version of its iPhone and iPad software will likely be the most important thing for the company to talk about. According to 9to5Mac, the next version of iOS will have a flat design. What does that mean? Well, it will shave off some of the textures you see around the software and apps.

"For example, the yellow notepad-inspired Notes app and Leather-bound Calendar interfaces on the iPhone and iPad will no longer be present," 9to5Mac's Mark Gurman reports. His sources also say that the casino game icons and design of Game Center will be wiped out.

iOS 7 is the first version of the software that has been worked on by Apple's chief designer Jony Ive. Ive replaced Scott Forstall in October 2012.

Beyond the design, there are said to be new native sharing capabilities tied in, similar to what is available now for Facebook and Twitter. Flickr and Vimeo are pegged to get tighter integration. There is also speculation that photo filter options will be added to the Camera app.

Do not expect to hear about or see a new iPhone or iPad at this event. Although, we might hear about Apple's rumored iPhone trade-in program.

Over the last couple of years Apple has continued to bring aspects of iOS to its Mac operating system, and the expectation is that there will be more of the same this year.

9to5Mac reports that there won't be major design changes to the software, but that Apple might add the app switcher from iOS to Mac for when users are in full screen mode.

Apple is also said to release some Mac hardware at the show. While the new rumored MacBook Air and Pro computers won't likely run the new software, they are said to be thinner and faster thanks to Intel's new Haswell chips. The new processors offer better battery life while providing faster processing power.

Earlier this week The New York Times reported that Apple is working hard to finalize music deals as to announce its streaming music and radio service at the event next week. According to that report, the service will compete with apps like Rdio, Pandora and Spotify with streaming radio based on your music preferences. It is said to be free and have integrated advertising.

An Open Letter to Microsoft About Windows Red

Dear Microsoft,

InfoWorld has reviewed your products for more than three decades. Some we've loved, like Windows 7 or Windows Server 2012. Others, like Windows

Vista or Windows 8, not so much.

Now, with the "release" of InfoWorld's Windows Red, we'd like you to review one of ours. Sure, Windows Red is a proposal rather than an actual product - an article plus a slideshow created by us - but the changes we've laid out are perfectly feasible. Perhaps some are already built into your Windows 8.1 upgrade, code-named Windows "Blue," due to arrive on June 26 (though the chances appear to be slight). Or you may believe Windows Red is a fatally flawed idea. Either way, go ahead: Turn the tables and let us know what you think.

You've said you're bringing back the Start button in Windows "Blue." In Windows Red, we've gone much further. Almost every reviewer has said the same thing: Windows 8 is two operating systems awkwardly bolted together and difficult for users to navigate. So in Windows Red, we've taken the obvious measure of separating them.

There's no other way to say it: Metro is a touch UI that has no business on a desktop or laptop screen. It's impractical to raise your hand from the keyboard to touch the screen and studies have shown it can be ergonomically harmful. On the flip side, a tablet should not be forced to run the traditional Windows Desktop, whose icons are too small for a touch interface and which demands so much power that Windows 8 tablets have been burdened by heavy batteries and short battery life.

Separation is good, but so is some degree of interoperability. Windows Red preserves the ability to run Metro apps on the desktop, including live tiles, but in a way that doesn't compromise the Windows Desktop experience. We also suggest you make Windows Phone and Windows tablet (Win8 and RT) apps binary compatible, so Metro apps can run on any Windows platform.

Beyond these fundamental fixes, the Desktop version of Windows Red proposes new capabilities, many inspired by Metro's own innovations: integrated sharing functionality, an improved Control Panel, a Desktop version of Windows Phone's People app, and a new grouping function for Desktop apps and folders. The Mobile version of Windows Red, based on Windows RT, ditches the unintuitive Charms bar, enhances the Applications bar, features a more flexible Snap View, and adds a much-needed Settings app. We also believe Microsoft should create a native Windows RT version of Microsoft Office designed specifically for touch.

We hope you take Windows Red in the spirit in which it was intended: a practical proposal for fixing Windows 8 rather than another harsh critique. Judging by previous user comments that have appeared on our site, we believe the basic tenets of Windows Red will be supported by many InfoWorld readers. No doubt they'll let us know. Meanwhile, Microsoft, we'd like to hear what you think.

Sincerely,

Eric Knorr
Editor in Chief, InfoWorld

Why Facebook No Longer Looks Destined To Take Over The Internet

Just a little more than a year ago, Wall Street s IPO hype machine went

into overdrive pushing Facebook as the next Google or Amazon that is, a company destined to branch out from its original mission to conquer a large segment of services on the Internet. But now that Facebook has been public for more than a year, its prospects becoming a Google or Amazon-style behemoth seem much more distant, Reuters reports. To be clear, there s little chance that Facebook will be like MySpace, which saw its user count completely crash over the span of a year in 2010, but there s also little sign that the company s ambitions to challenge Google in the search realm will ever bear any fruit.

What s more, Facebook faces a long-term challenge in competing against the plethora of messaging and photo-sharing applications that have popped up around the web in recent months. Facebook took one big potential competitor out of commission when it bought Instagram but that hasn t stopped new apps such as SnapChat from rising up seemingly overnight to become instant sensations. Chuck Jones, founder of technology research firm Sand Hill Insights, tells Reuters that Facebook could suffer death by a thousand SnapChats in three-to-five years if it can t keep pace with the frantic pace of innovation in today s mobile app market.

For the time being, though, Facebook has maintained its hold as the world s top comprehensive social network as competing services such as Google+ have remained comparative ghost towns. Whether the company will ever become anything more, however, is still very much up in the air.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.